Simplifying OT/IIOT Security

and Protecting against Cyber-Warfare

Kunal Agarwal

GM, Internet of Things

September 2018

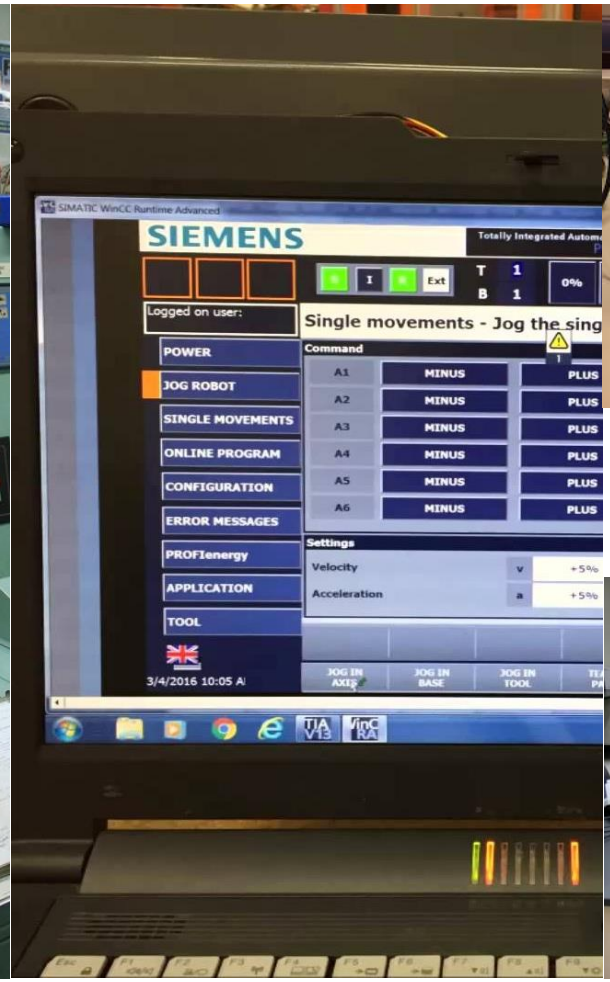
The Problem

Section
1

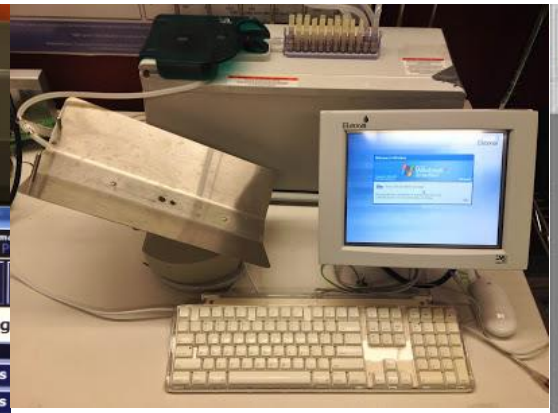
OT - Out of sight, out of mind.

Manufacturing

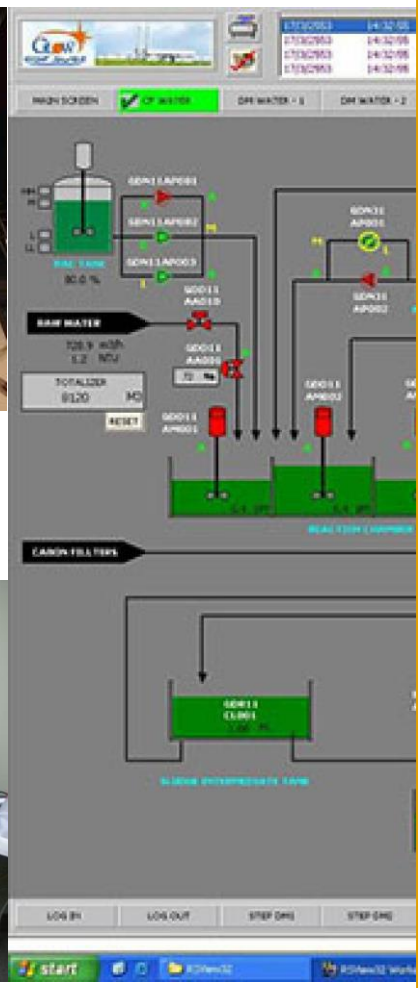
Ships



Automotive MFG



Pharma/Hospital



Oil/Gas

But not anymore…

triton

Industrial-scale safety instrumentation systems in Middle East targeted with vendor-specific attacks

0 Signatures at time of attack

USB Entry

3 Attack Options

Wannacry variant, halted production and may even cause delays on new iPhone shipping date

1+ Year Old Malware

SOP not followed

$300M USD

Attack Profile

The majority of infections are accidental. They use inherent vulnerability of the system to attack:

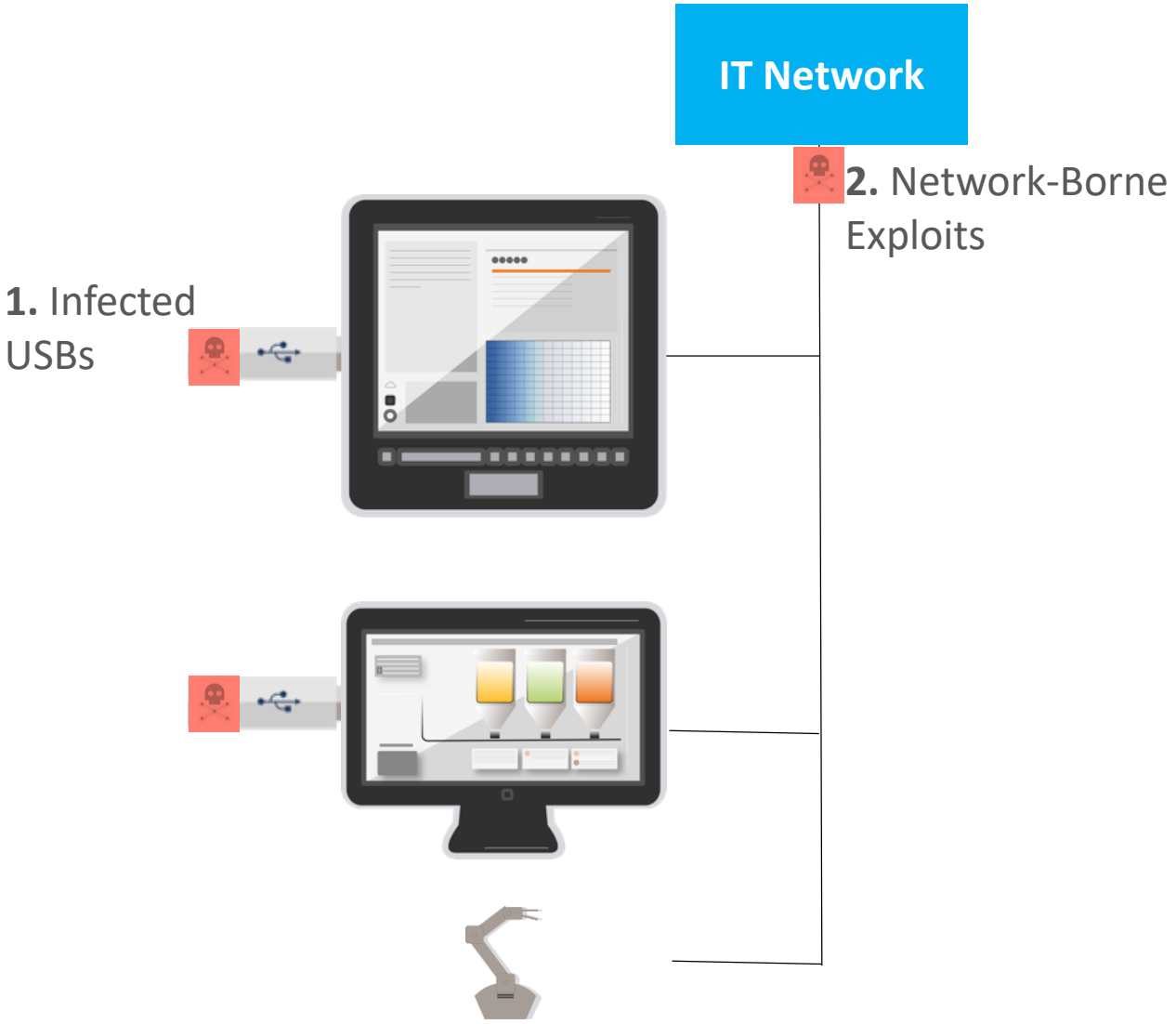
- EOL Operating System
- Content-based AV not suitable
- Valid OT Protocol Messages
- Airgap is not really an airgap

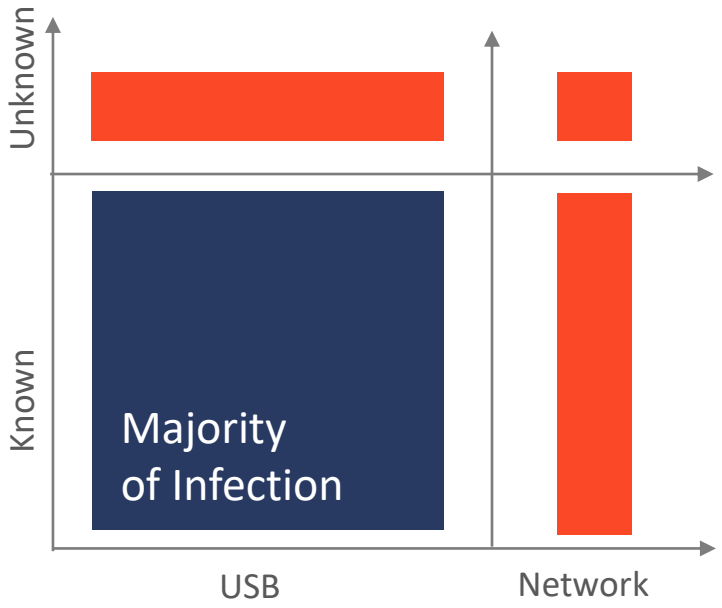
Intel gathering	Downtime to production	Invalid data display to operations	Invalid programming sent to controllers

What can we learn?

Section
2

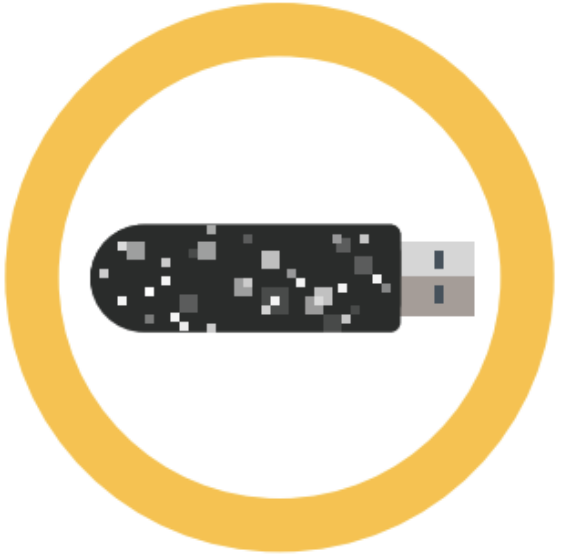
Research shows us very clearly:





2 Pain Points of Fixed Function Systems

WL + AE + Hardening



USB Washing Machine

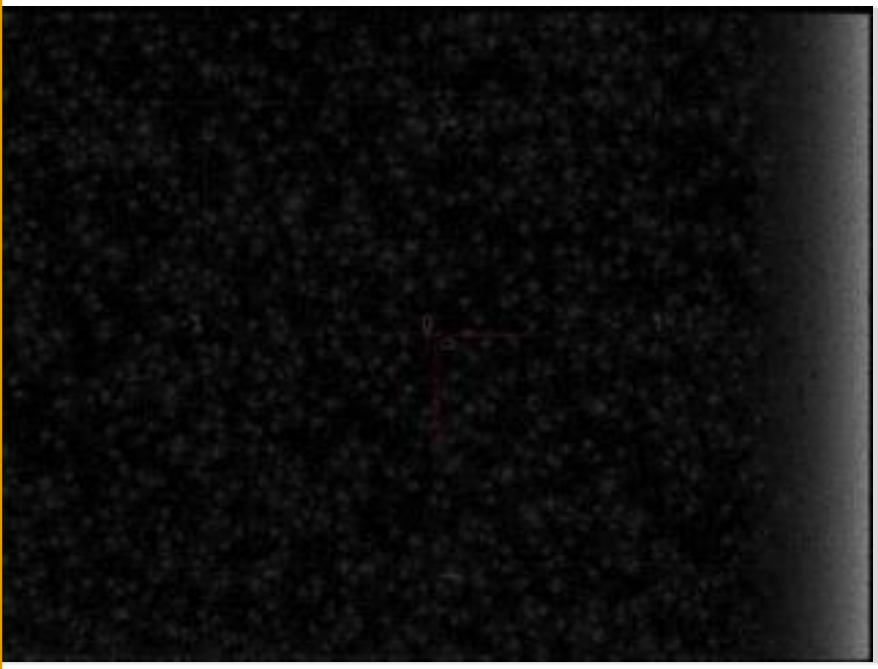
USB Washing Machine

1. Infected USB

2. USB Cleaning

3. Enforce only Cleaned USB

Machine Learning is Critical.



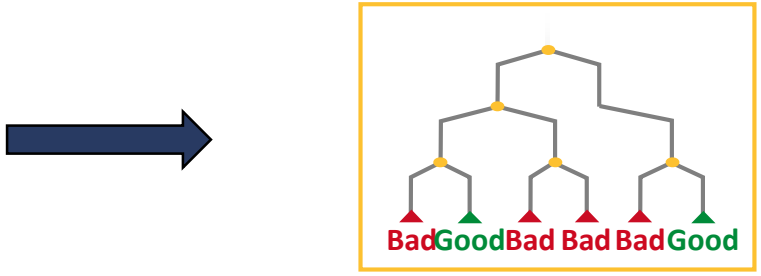
1. **Greater detection efficacy**

2. Extend expiration date without internet connection

3. Adversarial Machine Learning

4. Organic Self-Learning

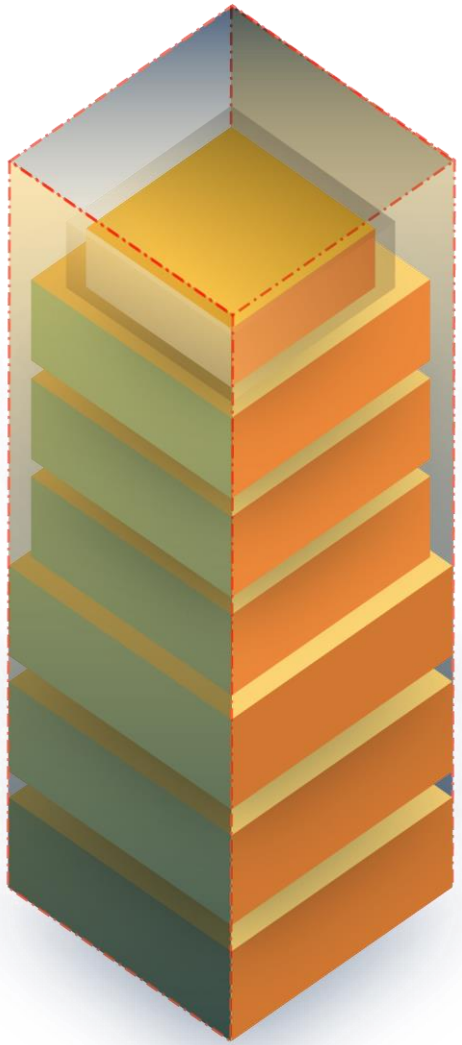
Features	Labels
14,67,191,1,001	Bad
27,93,159,0,101	Bad
13,22,120,1,011	Good



System Hardening

External Threats
Application vulnerabilities
Unpatched Applications

Internal Threats
Vulnerable Unpatched OS
Targeted Threats



Application WL+Isolation

Anti-Exploits

OS Hardening

USB Device Whitelisting

Network Firewall

Fundamentals:

1. broad compatibility
   - Even legacy windows OS like XP / 2000
2. anti-exploit
   - WL alone is not enough
3. OS hardening
   - No patches required to secure the operating system against attack
4. No Internet

Thank You!